SANS SECURING THE HUMAN

OUCH! | August 2015

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

Backup & Recovery

Overview

Sooner or later, you most likely will have something go wrong and lose your personal files, documents or photos. Examples include accidently deleting the wrong files, hardware failure, losing your laptop or infecting your computer. At times like these, backups are often the only way you can rebuild your digital life. In this newsletter, we explain what backups are, how to back up your data and develop a strategy that's right for you.

Guest Editor

Heather Mahalik is an industry-recognized forensics expert who focuses on smartphone forensics. She is co-author of Practical Mobile Forensics, technical editor of Learning Android Forensics and co-authors FOR585: Advanced Smartphone Forensics and FOR518: Macintosh Forensics for SANS Institute. Follow Heather at **Smarterforesnics.com** and on Twitter: **@heathermahalik**.

What to Back Up and When

Backups are copies of your information that are stored somewhere else. When you lose important data, you can recover that data from your backups. The problem is that most people do not perform backups, which is a shame because they can be simple and inexpensive. There are two approaches on deciding what to backup: (1) specific data that is important to you; or (2) everything, including your entire operating system. The first approach streamlines your backups and saves hard drive space; however, the second approach is simpler and more comprehensive. If you are not sure what to back up, then we recommend backing up everything.

Your next decision will be deciding how frequently to back up your data. Common options include hourly, daily, weekly, etc. For home use, personal backup programs, such as Apple's Time Machine or Microsoft's Windows Backup and Restore, allow you to create an automatic "set it and forget it" backup schedule. These solutions silently back up your data throughout the day while you are working on or away from your computer. Other solutions offer "continuous protection," in which new or altered files are immediately backed up as soon as they're closed. At a minimum, we recommend you back up daily. Ultimately, the question to ask yourself is, "How much information could I afford to lose if I had to restore from backup?"

How to Back Up

There are two ways to back up your data: physical media or Cloud-based storage. Physical media is any type of hardware, such as DVDs, USB drives or external hard drives. Whichever media you choose, never back up your files to the device that holds the original files. The problem with physical media is if your location has a disaster (such as a fire or theft), then not only can you lose your computer, but the backups, as well. As such, you should have a plan to store copies of your backup off-site in a secure location. If you do store them off-site, be sure you label them with what was backed up and when. For extra security, encrypt your backups.

Automated, reliable backups are often your last line of defense in protecting your data.

Cloud-based solutions are different. This is a service where your files are stored somewhere on the Internet. Depending on how much data you want to back up, this may be a paid service. It works by installing a program on your computer that automatically backs up your files for you. The advantage with this solution is that since your backups are in the Cloud, your backups are still safe if a disaster happens to your house. In addition, you can access your backups, or often even just individual files, from almost anywhere, even when traveling. The disadvantage is Cloud-based backups (and recovery) can be slower, especially if you have a large amount of data. If you are not sure which backup option is the best for you (physical media or Cloud) keep in mind you can always do both.

Finally, don't forget your mobile devices. The advantage with mobile devices is that most of your data is already stored in the Cloud, such as your email, calendar events or contacts. However, you may have information that is not stored in the Cloud, such as your mobile app configurations, recent photos and system preferences. By backing up your mobile device, not only do you preserve this information, but it is also easier to rebuild a device, such as when you upgrade to a new one. An iPhone/iPad can back up automatically to Apple's iCloud. Android or other mobile devices depend on the manufacturer or service provider. In some cases, you may have to purchase mobile apps designed specifically for backups.

Recovery

Backing up your data is only half the battle; you have to be certain that you can recover it. Check every month that your backups are working by recovering a file and validating the contents. In addition, be sure to make a full system backup before a major upgrade (such as moving to a new computer or mobile device) or a major repair (like replacing a hard drive) and verify that it is restorable.

Key Points

- Automate your backups as much as possible and check them regularly.
- When rebuilding an entire system from backup, be sure you reapply the latest security patches and updates before using it again.
- Outdated or obsolete backups may become a liability and should be destroyed to prevent them from being accessed by unauthorized users.
- If you are using a Cloud solution, research the policies and reputation of the provider and make sure they meet your requirements. For example, do they encrypt your data when it is stored? Who has access to your backups? Do they support strong authentication, such as two-step verification?

Protecting Your Personal Computer

Be sure to check out our free resources, including the blog and Video of the Month. This month, we're covering Protecting Your Personal Computer. View the video at http://www.securingthehuman.org/u/2uX.

Resources

Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Cloud Security:	http://www.securingthehuman.org/ouch/2014#september2014
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Tip of the Day:	http://www.sans.org/tip_of_the_day.php

License

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus